EXHIBIT A

LIEFF, CABRASHER, HEIMANN & BERNSTEIN, LLP
Kelly M. Dermody
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: (415) 956-1000
Fax: (415) 956-1008

JOSEPH SAVERI LAW FIRM, INC.
Joseph R. Saveri
500 Montgomery Street, Suite 625
San Francisco, CA 94111
Tel: (415) 500-6800
Fax: (415) 395-9940

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: HIGH-TECH EMPLOYEE ANTITRUST LITIGATION	Master Docket No.: 11-CV-2509-LHK
THIS DOCUMENT RELATES TO:	**CLASS ACTION**
ALL ACTIONS	**DECLARATION OF MELISSA BALDWIN, FOR HEFFLER CLAIMS GROUP, APPOINTED CLAIMS ADMINISTRATOR**

I, MELISSA BALDWIN, hereby declare:

1. I am employed as a Project Manager by Heffler Claims Group ("HCG"), the claims administrator in the above-entitled action. Our main office address is 1515 Market Street, Suite 1700, Philadelphia, Pennsylvania 19102. My telephone number is (267) 765-7402. I am authorized to make this declaration on behalf of HCG and myself.

2. Heffler Claims Group has extensive experience in class action matters, having provided services in class action settlements involving antitrust, securities fraud, employment and labor, consumer and government enforcement matters. HCG provided notification and/or claims administration services in more than 700 cases.

3. HCG was engaged by counsel for the parties as the Claims Administrator to provide notification and other services in connection with the settlement reached in the above-captioned matter (the "Settlement").

4. In order to perform the claims administration services as ordered by the Court, HCG anticipates the receipt of data files from the Defendants. These data files may include the following information for each Class Member that was employed by Defendant during the relevant Class Period: (1) full legal name, (2) social security number, (3) all known email addresses, (4) last known physical address, (5) dates of employment, and (6) associated base salary by date and relevant Class job title.

5. Due to the confidential and sensitive nature of the foregoing employment and personal information, HCG will expend great effort in securing and protecting the data. Numerous physical and logical policies and security controls are built into our infrastructure and applications allowing very granular, role-based security to be established, enforced and monitored. Examples include:

a) Application access is monitored and controlled using role-based functional security and activity logs. Access and functional controls are very granular, and each must be pre-authorized on a case-by-case basis by the Partner-in-charge of each case.

b) Computing and storage devices require pre-authorized role-based credentials for user access, and are protected from viruses and malware using endpoint security software. Internet access is secured and monitored using firewalls, security appliances, and endpoint security software. All laptops are encrypted and USB ports on workstations are blocked.

c) Data is also encrypted (using AES 256 encryption software) during transmission, and sensitive data is encrypted at rest in the database. Case-specific web sites designed to gather claimant data are secured via HTTPS technology, supplemented with security certificates as required by the case.

d) All data is encrypted prior to being backed up to tape and stored in a secure third-party off-site location. Secure tape transport between locations is provided by the storage vendor. Retired media (including hard drives) are destroyed by a certified third-party firm, with destruction certifications provided as required.

e) Sensitive data is prohibited from being stored on removable media devices, including laptop computers and external drives. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques. Unattended removable media devices must be physically secured by a lock and key (eg: locked office, locked drawer, locked file cabinet).

f) Building access is monitored and controlled by building personnel. Permanent residents receive a photo ID for identification and to activate elevators after normal business hours. Visitors must sign in and receive a photo ID badge when they enter our building. The Firm's receptionist is notified via e-mail from the lobby security that a visitor is on their way to our office. Visitors must sign in when they reach our reception area, are escorted to the office of the person they are visiting, and are signed out with the Receptionist when they depart. All entry doors to our office, with the exception of the reception area, are locked with key locks; the reception area is also locked after regular business hours.

g) Server Room access is monitored and controlled by IT personnel. Key distribution is limited to IT operations and supervisory personnel only. All visitors are accompanied by authorized personnel. Activity is monitored by cameras.

h) The claims processing area is highly secured with key entry access.

i) Paper case files are secured in locked file rooms or cabinets, accessible by pre-authorized individuals only.

6. The above standard practice policies and controls have been instituted in securing and protecting confidential and sensitive data received and/or accumulated during the claims administration of over 100 securities, antitrust, consumer and employment matters handled by HCG.

7. HCG agrees that all sensitive data, including, but not limited to, Social Security Numbers and salary information, will be stored and maintained on a secure server at all times. The storage of this data on laptops or other mobile devices will be strictly prohibited.

8. HCG believes that these policies and controls are state of the art for data privacy in the industry.

9. In the history of our claims administration work, HCG has no record of any data breach and/or security incident in which sensitive, protected or confidential data has been copied, transmitted, viewed, stolen or used by an individual/entity unauthorized to do so.

10. HCG will destroy all data from this matter when the notice and claims administration process is completed.

I declare under the penalty of perjury, under the laws of the State of California, that the foregoing is true and correct and that this declaration was executed on October 25, 2013, at Philadelphia, Pennsylvania.

MELISSA BALDWIN